Chris Oakes
Oct 22, 1999 12:00 PM
Wired News

Monitor This, Echelon

Privacy advocates may not have been able to stop the snooping, but making their intrusion-jamming efforts highly public may have done some good after all. If you forgot to mark it on your calendar, Thursday was the day to jam international communications systems tracking your every word. Activist hackers conceived Jam Echelon Day under the […]

Privacy advocates may not have been able to stop the snooping, but making their intrusion-jamming efforts highly public may have done some good after all.

If you forgot to mark it on your calendar, Thursday was the day to jam international communications systems tracking your every word.

Activist hackers conceived Jam Echelon Day under the premise of: If we're being monitored, let's really give them something to monitor.

The email-based campaign came amid expanding conjecture that superpower world governments may have constructed a massive global system for monitoring all electronic communications -- the mysterious, undocumented system known as Echelon.

"Today is officially the first annual day [that] the world is invited to protest our global surveillance by the spooks at Echelon, the global communications monitoring system that has been set up to keep an eye on all our potentially subversive business, social, personal and other communications," read an invitation sent to subscribers of the Hacktivism email list.

According to the message, participants were encouraged to "pass a few of the keywords sought by the Echelon systems by phone, fax, or email to someone else in hopes of first making a blip of protest on the Echelon radar and later, perhaps, even crashing the system."

The near-mythical worldwide computer spy network reportedly scans all email, packet traffic, telephone conversations, and more in an effort to ferret out potential terrorist or enemy communications. Once a communication is plucked from the electronic cloud, certain keywords allegedly trigger a recording of the conversation or email in question.

Use at least one email with at least 50 keyword words, such as "revolution" or "manifesto" or "revolt," organizers suggested. Various civil liberty and activist groups have made their own trigger suggestions. These include the following red flags:

ATF DOD WACO RUBY RIDGE OKC OKLAHOMA CITY MILITIA GUN HANDGUN MILGOV ASSAULT RIFLE TERRORISM BOMB DRUG KORESH PROMIS MOSSAD NASA MI5 ONI CID AK47 M16 C4 MALCOLM X REVOLUTION CHEROKEE HILLARY BILL CLINTON GORE GEORGE BUSH WACKENHUT TERRORIST.

Although organizers said it was hard to tell if the theoretical sniffing system was affected, observers monitoring hacker lists and activism sites detected a fair degree of participation.

"People are sending emails with what they think are keywords and trying to trigger it," said the webmaster of the respected hacker journal, 2600, who identifies himself by the handle Macki. He said it was very difficult to quantify participation, but guessed that the event saw at least thousands of participants. "[People are writing] 'Yeah -- I jammed Echelon,' and putting half a dozen keywords in their email, and on the Hacktivism mailing list," Macki said.

Privacy activists have put triggering words in their signature files in the past, but activists wanted to trip up Echelon in a more significant way. They hoped the event, also referred to as "gag Echelon day," would catch on with global scale and raise awareness of the alleged system.

One non-hacker participant who added the words to his email Thursday was 75-year-old World War II veteran Everett E. Slaughter. "I remember the oath I took when I joined the military in 1942. I took an oath to defend the Constitution," he said. "I still honor that oath."

The US Constitution guarantees the right of privacy, and that should extend to fax, email, and telephone communications, Slaughter said. "I think we need to honor those things."

While 2600's Macki respects the idea of raising awareness of the potential dangers of a system like Echelon, he said the hacktivist community's good intentions were a bit misguided.

"It's all very vague and people don't know about how Echelon works," said Macki. "So a focused effort like this to trip it up can't have any more than limited success." The campaign should have exploited the chance to increase awareness of a technology truly capable of defending against all Echelon-like threats: encryption.

If participants began encrypting all the email and other data flowing out of their PCs, the taxing job of decrypting would have been more likely to thwart electronic monitoring, Macki said.

Last fall, the Washington-based conservative public policy think-tank Free Congress Foundation sent a detailed report on Echelon to Congress, but the system has not yet been debated on the floor. The foundation hopes that Thursday's efforts will help make that happen.

Lisa Dean, vice president for technology policy at the Free Congress Foundation considered Jam Echelon Day a great way to focus attention on the issue.

"I agree that Thursday's campaign is unlikely to jam Echelon. But this is an extremely effective and clever PR campaign that the hackers are putting on. Because Americans largely don't know what Echelon is. And then all these reputable people like [Congressman] Bob Barr [R-Georgia] are talking about Echelon."

Dean said Barr's interest would ensure that Congress will hold hearings on the issue next year.

Neither the National Security Agency (NSA) nor its UK equivalent -- the Government Communications Headquarters -- has admitted that the system exists, although its feasibility and characteristics have been debated in the European Parliament. Australia's Defense Signals Directorate, an agency allegedly involved in Echelon, recently admitted the existence of UKUSA, an agreement between the five national communications agencies that reportedly governs the system.

2600's Macki, for one, thinks Echelon is no longer a far-fetched notion.

"It's been very well documented by the European parliament, and other groups. Intelligence agencies are interested in a very broad range of subjects."

The flap over Echelon highlights the broader issue of intelligence communities spying on their own citizens, Macki said. Echelon is the perfect solution for an otherwise illegal activity. "It's like Australia is spying on US citizens, then passing that off to US intelligence agencies ... it's kind of a mutual way of getting around spying on ourselves -- which is of course illegal.

The Free Congress Foundation's Dean is holding off validating Echelon's existence.

"I'm not ready to come out and say all our communications are being intercepted," she said.

"But the possibility is there and certainly the capability."

###